ELECTRONIC PRIVACY INFORMATION CENTER

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of
ACA International Petition for Expedited Clarification
Docket No. 02-278

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
May 11, 2006

The Electronic Privacy Information Center is pleased to submit comments to the Federal Communication Commission on ACA's International (ACA) Petition.

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has filed a number of comments to the FCC on matters of concern to consumers and as an advocate for consumer privacy protection. In January of this year we filed comments for a declaratory ruling filed by the Fax Ban Coalition that encouraged the FCC to reject an attempt by a petitioner to preempt California and other states superior protection against junk faxes. In April 2004, in a matter that was before the Commission on unwanted mobile service commercial messages and the CAN-SPAM Act our comments stated that Congress in its wisdom did shield wireless devices from automatic dialers, prerecorded and artificial voice communications.

Background

On December 20, 1991 the Telephone Consumer Protection Act of 1991 (TCPA) became Public Law 102-243. The TCPA prohibits any person within the United States or internationally from using an automatic telephone dialing system (ATDS) or an artificial or prerecorded voice (APV) to make a call. Further, the law stated that any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or radio common carrier service or any other service for which the called party is charged for the call; or initiating any call to a residential telephone line using an APV to deliver a message without the consent of the called party was prohibited.

Their users consider wireless communications devices highly personal. Millions of individuals carry wireless devices everywhere they go. In part, the success of wireless devices and users' trust in them can be attributed to their status as a safe haven from telemarketing. Individuals trust that when their wireless phone rings, a friend or family member will be on the line, rather than a telemarketer. This trust in wireless service was created by Congressional action. In 1991, Congress passed the Telephone Consumer Protection Act, which created protections both for residential and wireless phone services.[i] Specifically, Congress flatly prohibited the use of autodialed, prerecorded voice, and artificial voice telemarketing to paging services, cellular telephone services, or any service for which the called party is charged for the call.[ii] Other services found to deserve the same level of privacy protection included emergency "911" lines and hospital rooms.[iii] As a result of Congress' action, generally, wireless telephones do not receive telemarketing calls.

The Petitioner

The ACA founded in 1939, is an industry lobby comprised of more than 5,500 members worldwide, including third-party collection agencies, asset buyers, attorneys, creditors and vendor affiliates. The ACA asks the Federal Communications Commission (FCC or Commission) to exempt debt collectors from cell phone privacy rules adopted under the Telephone Consumer Protection Act (TCPA).[iv]

I. In Passing the TCPA, Congress Clearly Demonstrated an Intent to Bar ATDS

Congress was explicit in the language of this law--Section 227 (b) Restrictions on the Use of Automated Telephone expressly prohibits the use of ATDS from making any calls to "to any telephone number assigned to a paging service cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call."

The language of the law leaves no doubt about Congressional intent—to address the growing privacy threat to consumers posed by the automation of telecommunication technology and specifically to address the growing problem of ATDS. The total capacity for generating calls in 1991 was estimated to be more than 18,000,000 households each day. Consumers reacted to the growing invasion of their privacy and Congress acted by passing this law.

The Telephone Consumer Protection Act directed the Federal Communications Commission (FCC)[v] to prescribe regulations to implement such requirements. Directs the FCC to: (1) initiate a rulemaking proceeding concerning the need to protect residential telephone subscribers' privacy rights to avoid receiving telephone solicitations to which they object; and (2) prescribe regulations to implement methods and procedures for protecting such privacy rights without the imposition of

any additional charge to telephone subscribers. States that such regulations may require the establishment and operation of a single national database to compile a list of telephone numbers of residential subscribers who object to receiving such solicitations, or to receiving certain classes or categories of solicitations, and to make the compiled list available for purchase. Outlines information to be included in such regulations if the FCC determines that such a database is required.[vi] The Do-Not Call Registry is the result of the work done by Congress beginning in 1991 to protect consumers from the foreseeable conclusion of the joining of computing and telecommunications technologies. . However, it was not until January 22, 2002 that the Federal Trade Commission (FTC) solicited comments for the creation of the first national Do-Not Call registry.[vii]

Part of the work of the FTC in managing the Do-Not Call registry is to work with the FCC in your enforcement activities.[viii] This registry is by far the single greatest indicator of the desire of the American public to be free of unwanted telephone solicitations. During FY 2003 and FY 2004 over 64 million numbers were registered, and the data shows good compliance records by telemarketers.

Congress also spoke on the use of APV messaging by directing the FCC to prescribe technical and procedural standards for these systems transmitting APV messages via telephone that require: (1) the messages to clearly state the identity and telephone number or address of the entity initiating the call; and (2) such systems to automatically release the called party's line within five seconds of the time the party has hung up.

Provides that if the FCC requires the establishment of a database of telephone numbers of subscribers who object to receiving telephone solicitations, a State or local authority may not require the use of a database or listing system that excludes the part of the national database that relates to such State

II. The Reality of Identity Theft is a Further Challenge that the Commission Must Consider When Debt Collectors Seek Exceptions to the Law

In 2002, identity fraud is estimated to have cost $53 billion and over 297 million hours for nearly 10 million victims of identity theft.[ix] The argument posed by the ACA that they only seek to collect outstanding debt must be weighted against the reality of identity theft. Identity theft in the form of credit card fraud, new account fraud, identity cloning, or criminal identity theft; most often only involves three persons the victim, the imposter, and the creditor.[x]

In a survey of more than 4,000 Americans, the Federal Trade Commission found that identity theft cost victims $5 billion in out-of-pocket expenses, and nearly 300 million hours of their time trying to fix damage caused by the crime. The FTC

survey showed that in all, 27.3 million Americans were affected by identity theft in the previous five years. The cost to businesses for this same period is estimated to have been $47.6 billion.

The FTC found that 49 percent of all the 4057 respondents did not have any idea whatsoever how their identity came to be purloined, while 22 percent cited theft and another 12 percent claimed the information was stolen in the course of a transaction.

The welcome mat is out from thieves to gain access to valuable personally identifiable information of consumers. Personal information can be stolen from a company, for instance, from a corrupt employee. Personal information is often thrown away by careless businesses. Impostors then dig through the trash and find the information. A data broker could sell information to criminals, as was the case with ChoicePoint. Many key identifiers used in credit granting can be found in public records. Friends, roommates, and family members can access information for the purpose of identity theft.

EPIC along with other consumer privacy enhancing institutions have long advocated that the door be closed and locked against access to personal information. We believe that the credit lenders who use a flawed, circular system to identify and authenticate individuals should take the full cost of identity theft.[xi] Unfortunately, the core problem in identity theft is that a business cannot discern the difference between the impostor and the victim using the faulty means of authenticating borrowers. This problem has its roots in the credit granting process--the same information that is used to identify the credit applicant is used to "authenticate" her.

Identification is the process of placing a label on an individual ("I am John Doe"). Authentication is the process of verifying the label. That is, proving that one is who she claims to be ("This document proves that I am John Doe"). Many different things can be used for authentication. For instance, a password can be used to verify that one is authorized to use a computer account. Tokens are also used for identification. For instance, a bus token can prove that one has authority to ride the bus.

But creditors don't use sound authentication methods. They use your personal information as a password—the same personal information you use to identify yourself.

Should the Commission grant the petition in this case the time and cost to consumers may increase exponentially. It is our conclusion that the Commission properly interpreted Congress' intent in its rule that bars the use of ATDS and APV technology as a means of sending communications to all telecommunication devices.

III. "Express Prior Authorization" Should Be in Writing

In the course of permissible communications as dictated by the TCPA creditors should be directed to obtain express prior authorization from customers in writing, recipients will face an extremely difficult hurdle in enforcing these regulations. It has been our experience from communication with junk fax litigants that junk fax broadcasters frequently claim that the recipient opted in to the transmission. At that point, the individual is forced to prove a negative that consent had not been given at any time in the past. This is often an impossible challenge for litigants. Any number of thousands of transactions could have included language creating an existing business relationship or some consent to receiving the messages. A previous holder of the telephone number could have consented. Or the individual's family members may have consented. The Commission should not place consumers in the same situation when attempting to enforce their rights against senders of aggressive debt collection tactics. Affirmative consent should be in writing. That will shield legitimate communications from frivolous litigation and will assist individuals when their rights have been violated

IV. There Should Be No Exemption for Providers of Commercial Mobile Services

Polling in the area of privacy shows that people want less, not more, spam.[xii] It makes little difference if the sender is a legitimate company, an illegitimate company, or even a company with which individuals regularly transact.

If the Commission chooses to create an exemption for commercial mobile services providers, the burden will be upon individuals to opt out. Again, opt-in is a more efficient solution for individuals, because telephone carriers have so poorly implemented opt-out mechanisms that it appears as though they are attempting to frustrate individuals' choices.

For example, Verizon may have the worst opt-out implementation that EPIC has ever encountered. In order to opt-out of CPNI sharing from Verizon, one must first notice the privacy notice that appears on the last page of customers' statements. The policy never mentions the word "privacy," and instead is titled "Customer Proprietary Network Information - Special Notice." Additionally, the opt-out policy never specifies that "Customer Proprietary Network Information" refers to calling records-a detailed list of every call an individual makes. This notice is vague and does not adequately inform consumers of the nature of the information collected or the significance of failing to opt-out.

Furthermore, Verizon customers who have attempted to opt-out have encountered a cumbersome and confusing process. Individuals must provide their phone number, their account number, the name on the account, their address, and speak the name

of the "authorized" person to make decisions on the account. This process places an unreasonable burden on consumers who simply wish to protect their privacy. Further, the script used by Verizon to guide consumers through the opt-out process employs language that discourages individuals from exercising their rights. For instance, when a consumer chooses to opt-out, the script responds, "You are requesting to establish a restriction on your account"--a characterization that misleads customers about the ramifications of their decision.

We ask that the Commission reject the petition in light of the language of the authorizing statue and the need to protect consumers from unwanted and invasive communications.

Respectfully submitted,

Lillie Coney
Associate Director
Electronic Privacy Information Center

---

[i] Public Law 102-243, 47 U.S.C. § 227.
[ii] Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 69 Fed. Reg. 16873 (Mar. 31, 2004).
[iii] Id. at (b)(1)-(2).
[iv] Hundreds of ACA's member companies have filed comments with the FCC supporting the Petition. Member comments are largely repetitious and do not outweigh the underrepresented consumer perspective.

[v] Library of Congress Summary of S. 1462 the Telephone Consumer Protection Act of 1991
[vi] Do-Not Call Registry, see: https://www.donotcall.gov/default.aspx
[vii] EPIC's Do-Not Call Registry Status Page, see: http://www.epic.org/privacy/telemarketing/dnc/
[viii] FCC Report to Congress for FY 2003 and 2004: Pursuant to the Do Not Call Implementation Act on Implementation of the National Do Not Call Registry
[ix] Congressional Quarterly, Identity Theft: Can Congress Give Americans Better Protection, June 10, 2005.
[x] See, EPIC's Identity Theft Web Page, http://www.epic.org/privacy/idtheft/
[xi] il
[xii] FTC, Email Address Harvesting: How Spammers Reap What They Sow (November 2002) at http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm.